Invasão de Privacidade

As primeiras invasões cibernéticas e seus marcos

- Contexto inicial (décadas de 1960–1970):
    - As primeiras ações digitais surgem no ambiente universitário e militar, com experimentos em redes de computadores (ARPANet/ARPANET). Entre os “hackers” iniciais estavam pessoas que exploravam sistemas para entender, brincar ou demonstrar vulnerabilidades. A ideia de “hack” ainda era associada a curiosidade técnica e à criação de soluções, antes de se tornar uma prática criminosa coordenada.
    - A prática de “phreaking” (exploração de redes de telefonia para chamadas gratuitas) já existia e influenciou o início da cultura hacker. Um nome recorrente nessa era é John Draper, conhecido como Captain Crunch, ligado a atividades de engenharia de som e manipulação de sistemas de telecomunicações.
- O marco técnico de maior impacto inicial: o worm Morris (1988)
    - O worm de Morris, criado por Robert Tappan Morris, é amplamente citado como o primeiro worm de computador que se espalhou pela internet de forma significativa. O incidente expôs vulnerabilidades de sistemas.

1) Visão geral e contextos-chave (2002–2026)

- Evolução da ameaça: de incidentes pontuais a ataques globalizados, com alta sofisticação, uso de ransomware, supply chain (cadeia de suprimentos) comprometida e exploração de vulnerabilidades críticas.
- Motivação dominante: lucro financeiro (ransomware, exfiltração de dados), espionagem, sabotagem e coerção. Atingem setores críticos (energia, financeiro, governo, saúde) e plataformas empresariais amplas.
- Desafio de atribuição: muitos ataques são atribuídos com grau de incerteza; atores podem usar técnicas de disfarce e operações em nuvem para dificultar identificação.

2) Casos marcantes por períodos (2002–2026)

- 2003–2004: ataques de botnets emergentes, com foco em discrições de fraude e spam, abrindo caminho para a monetização de redes de zumbis.
- 2007–2008: ataques de botnets de grande escala e campanhas de malware bancário; evolução para técnicas de rootkits e exfiltração de dados financeiros.
- 2010: Stuxnet (Iran/Irã) – malware sofisticado visando centrifugadoras de urânio; exemplo de ofensiva cibernética de estado com consequências industriais.
- 2013–2014: ataques a varejo e instituições financeiras com exfiltração de dados em larga escala (frequente violação de dados de cartões de crédito).
- 2014–2015: primeira onda significativa de ransomware com impacto corporativo; crescimento de ransom em setores de saúde e manufatura.
- 2016: NotPetya – devastador indiscriminado com disfarce de ransomware, amplamente creditado como ataque destrutivo com destruição de dados e interrupção empresarial global.
- 2017: WannaCry e NotPetya continuam gerando lições sobre vulnerabilidades de SMB (MS17-010) e cadeias de suprimentos.
- 2018–2019: invasões em cadeias de suprimentos (com principal foco em software de terceiros) e ataques de ransomware com reajuste de pagamento exigido em criptomoedas.

- 2020: pandemia global amplifica ameaças remotas; ataques a assistência médica, serviços públicos, empresas com aumento de teletrabalho.
- 2020–2021: SolarWinds – ataque de cadeia de suprimentos de alto nível, comprometendo clientes corporativos e agências governamentais; uso de várias ferramentas de intrusão e malware sob medida.
- 2021–2022: ataques a infraestrutura crítica (oleodutos, energia) com interrupções significativas; ataques de ransomware com exigência de pagamento elevado; aumento de crimes cibernéticos patrocinados por estados.
- 2022: vulnerabilidade Log4j (Log4Shell) expõe milhões de sistemas; ressalta a importância da gestão

1. **Windows (PCs e servidores)**
    - Por que é atacado com mais frequência: domínio de mercado no desktop e vasto ecossistema corporativo, histórico de vulnerabilidades divulgadas e ampla superfície de ataque.
    - Exemplos de vetores comuns: malware deWindows, exploits de vulnerabilidades de software, phishing direcionado, ransomware.
2. **Android (dispositivos móveis)**
    - Por que é atacado com frequência: grande base instalada, lojas de apps e permissões de sistema permitem exploração de permissões e apps maliciosos.
    - Vetores comuns: malware em apps, sideloading, falsificação de apps, exploits de componentes do sistema.
3. **Linux (servidores e dispositivos embarcados)**
    - Por que é atacado: uso extensivo em servidores, nuvem e infraestruturas críticas; muitas distribuições rodam serviços expostos.
    - Vetores comuns: operações de botnets, vulnerabilidades de serviços (SSH, web servers), exploração de vulnerabilidades no kernel/softwares de servidor.
4. **iOS (dispositivos móveis da Apple)**
    - Por que é atacado: forte mercado móvel com alto valor, atualizações rápidas e cadeias de confiança; ataques geralmente mais sofisticados e menos frequentes, porém de alto impacto quando ocorrem.
    - Vetores comuns: vulnerabilidades zero-day, malwares disfarçados de apps, exploração de componentes do sistema.
5. **macOS (computadores Apple)**
    - Por que é atacado: base de usuários crescente em ambientes domésticos e corporativos, evolução de malware específico para macOS.
    - Vetores comuns: trojans, adware/PUA, exploits de software de terceiros e kernel extensions.
6. **Sistemas embarcados/IoT (variações de RTOS e Linux embarcado)**
    - Por que é atacado: grande número de dispositivos conectados com segurança fraca, atualizações inconsistentes.

- Vetores comuns: firmware vulnerável, senhas padrão, exploração de serviços de rede expostos (Telnet/SSH, HTTP).

2. **Outros sistemas Unix-like e específicos (ex.: BSD, AIX, Solaris)**
    - Por que é atacado: menos comuns que Windows/Linux, porém presentes em ambientes corporativos críticos; ataques mais especializados podem ocorrer contra serviços específicos.
    - Vetores comuns: falhas em serviços de rede, exploração de software legado.

Microsoft e a coleta de dados

Dados de conta e configuração

Informações da Conta Microsoft (perfil, preferências, configurações de segurança, opções de idioma).

Dados de autenticação e uso de recursos vinculados à conta (logins, dispositivos conectados, preferências de privacidade).

Dados de diagnóstico e uso (além da telemetria básica)

Logs de erros, falhas e desempenho de software.

Dados de uso de recursos

Resumo por nível de risco (2026)

Posição	Distribuição	Nível de Risco	Principal Fonte de Coleta
1º	Ubuntu / Ubuntu Pro	Alto	Snapd, Whoopsie, Ubuntu Advantage
2º	RHEL / clones corporativos	Alto	Red Hat Insights
3º	Fedora	Médio-Alto	ABRT, Fedora Telemetry
4º	SUSE / SLE	Médio-Alto	SUSEConnect
5º	ChromeOS Flex	Muito Alto	Telemetria do Google
6º	Pop!_OS	Médio	COSMIC + Ubuntu base

Existem **vulnerabilidades reais** em **PAM** (Pluggable Authentication Modules) e **udisks** que permitem **escalonamento de privilégios** (privilege escalation) em várias distribuições Linux.

Detalhes:

- **PAM**:
  Vulnerabilidades no PAM podem permitir que um usuário local sem privilégios execute código com permissões de **root**. Isso geralmente ocorre devido a configurações incorretas ou falhas em módulos específicos do PAM.

- **udisks**:
  O **udisks** (usado para gerenciar discos e dispositivos de armazenamento) já teve falhas que permitiam que usuários comuns montassem dispositivos com permissões elevadas, o que poderia ser explorado para escalar privilégios.

Exemplos reais:

- CVE-2023-4911 (**"Looney Tunables"**): Falha no **glibc** (não no PAM diretamente), mas explorada em conjunto com configurações do PAM em várias distribuições.
- CVE-2021-3560: Vulnerabilidade no **Polkit**, que pode ser combinada com falhas no PAM.
- Falhas no **udisks2** já foram reportadas permitindo montagem de dispositivos com privilégios

Nos anos anteriores a 2026 eu havia ultilizado o Ubuntu / Ubuntu Pro, e por coincidência foi atacado,também cheguei a ultilizar o fedora,mesmacoisa,agora estou usando o arch linux e adivinha?

Mais de 1.500 pacotes do AUR do Arch Linux são comprometidos por malware

Mantenedores trabalham para remover o conteúdo malicioso e banir as contas afetadas. O incidente parece restrito ao AUR e não afeta pacotes oficiais do Arch Linux. Também foi identificado um segundo ataque, com um malware mais sofisticado que usa ofuscação de código, afetando projetos como bibliotecas de Node.js, applets do Plasma 6, componentes do Firefox, o navegador Aura, extensões do LibreWolf e um plug-in do NeoVim.

https://static.vivaolinux.com.br/noticia/ataque-a-cadeia-de-suprimentos-atinge-1-500-pacotes-do-aur-e-leva-arch-linux-a-congelar-novos-cadastros/

https://www.reddit.com/r/LinuxTurkey/comments/1u4bsfb/1500den_fazla_aur_paketi_zararl%C4%B1_g%C3%BCncellemeler/?tl=pt-pt